X2000/IFDP System Engineering Process for Risk Management[1][2]

DRAFT Version

Tom Hoffman
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena , CA 91109
818-354-6521
Tom.L.Hoffman@jpl.nasa.gov

Cecilia Guiar
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena , CA 91109
818-354-6756
Cecilia.N.Guiar@jpl.nasa.gov

Abstract—This paper describes some of the processes employed by the X2000/IFDP system engineering team to manage risk. This paper will describe the difficult system engineering task undertaken by the X2000/IFDP team of trying to develop a technology rich avionics system for a divergent interplanetary mission set. The ability to balance the risks inherent in technology development against the tight requirements of interplanetary missions was the job of the system engineering team. This job posed a unique set of challenges for the team requiring that new processes be developed.

Many of the successful processes employed by the X2000/IFDP System Engineering team will be discussed in detail. The bottom line of each of the processes involved early and deep involvement by each of the affected subsystems. This allowed the system design issues to be worked in sufficient detail that the requirements and associated risks could be clearly identified.

TABLE OF CONTENTS

1. INTRODUCTION
2. X2000/IFDP SYSTEM DEVELOPMENT TENETS
3. MISSION CUSTOMER SET
4. X2000/IFDP SYSTEM DESCRIPTION
5. SYSTEM RISK MANAGEMENT PROCESSES
6. SYSTEM PROCESSES DESCRIPTION
7. CONCLUSIONS

1. INTRODUCTION

The paper will discuss the system engineering processes used on the X2000 Integrated First Delivery Project (X2000/IFDP). The X2000/IFDP hardware/software avionics system is being developed at NASA's Jet Propulsion Laboratory (JPL) to support multiple missions in the early 21st century. The set of missions range from deep space to earth orbiting with large differences in requirements. These many and often conflicting requirements required the system engineering process to be modified from the standard JPL approach. The main focus of this paper will be to describe the current system engineering processes in place for risk management.

The paper will first provide a background on the current set of mission customers that X2000/IFDP is supporting. The key requirements of these missions on the X2000/IFDP system will be summarized. This background is important to understand the wide variety of mission requirements imposed on the hardware and software avionics system. The X2000/IFDP system design will then be described to set the context for the discussion of system processes. The next section will describe the specific processes used by the system engineering team to manage risk on the X2000/IFDP project. These risk management processes were inherent in the overall system engineering process.

2. X2000/IFDP SYSTEM DEVELOPMENT TENETS

The key tenets of X2000/IFDP are identified below:

1) To enable/support low cost development and delivery of deep space missions;
2) To develop an architecture that is scaleable, modular, and upgradeable. The goal is to develop a standard core and to maintain a flexible set of building blocks which our customers can tailor to their needs;
3) To develop a design that is testable in a variety of testing environments. X2000/IFDP will have numerous test platforms;
4) To provide multi-mission support. The goal is to develop architectural concepts to accommodate the known set of mission needs. This is addressed more below; and
5) To enable the Europa Orbiter mission. Also addressed further below.

Developing a common suite of advanced avionics for

[1] 0-7803-6599-2/01/$10.00 © 2001 IEEE
[2] Updated 10/27/00

multiple missions that satisfies these key tenets in a timely manner is extremely challenging and required the system engineering element to be approached in a different manner.

3. Mission Customer Set

Numerous flight missions were surveyed in order to develop the requirements set to which the X2000/IFDP avionics system would be targeted. These missions covered a wide range of targets, science goals and environmental conditions.

The main and first customer of the X2000/IFDP avionics systems will be the Europa Orbiter (EO), currently scheduled to launch in 2006. EO will be exposed to 10 Mrad of radiation behind 40 mils of aluminum, while other missions are well under 100 krad. The EO mission also requires high data rate telecommunications to recover the science data within it's brief 30 day lifetime on orbit.

A companion customer to the EO was Pluto/Kuiper Express (PKE). PKE was initially intended to be similar in physical design to the Europa Orbiter. PKE was planned to operate out beyond 40 AU (0.0006 times the solar incidence at Earth), a driver on the thermal as well as the telecom requirements. At the other thermal extreme was our other potential customer, Solar Probe, which is planning on operating within 4 solar radii of the sun (3,000 times the solar incidence at Earth).

The New Millennium Space Technology 4 (ST-4) mission was another customer whose requirements were incorporated. The ST-4 was to be a cometary lander with very tight power constraints. Additionally, Mars missions and the Space Interferometry Mission were also surveyed.

Europa Orbiter

Jupiter's moon Europa fascinated scientists after the images from the Voyager Mission indicated that the surface of Europa was unusually smooth and lacked visible craters, suggesting that it was very young. Combined with information about its bulk composition, which indicated it had a veneer of water ice, and the knowledge that Europa experienced strong, heat inducing tides, this finding led to the tantalizing suggestion that a water ocean might be present below the moon's surface. The data were of insufficient resolution to allow much more than theoretical speculation, and the Galileo observations were awaited with eagerness.

The Galileo images did not disappoint. In a June 1996 image, strong evidence appeared for surface cracking into ice floes, reinforcing a Voyager interpretation. Then the close Europa flybys found the first direct evidence of cryovolcanism on a Jovian moon. These were followed quickly by apparently clear evidence of what appear to be icebergs now apparently frozen into place, but which appear to have been floating on some substrate that is difficult to conceive of as anything but liquid. But while increasingly compelling, there was as yet no unequivocal determination of the existence of a global ocean on Europa.

About the time of these discoveries, the Jet Propulsion Laboratory began advanced studies of the EO mission which would determine if an ocean is present and the thickness of the overlaying ice layer.

The current plan for the Europa Orbiter would take about three years to reach the Jovian system and an additional one and a half years to reach orbit around Europa. The mission consists of one month in orbit around the moon taking data and relaying the data back to Earth. The mission duration is driven primarily by the intense total ionizing dose radiation levels present in the Jovian system.

The proposed Europa science suite features a radar sounder to remotely determine the depth of the surface ice and determine if a liquid water ocean exists beneath it. Visible and thermal imaging is also included to map the surface and determine composition and structure. Accurate tracking of the spacecraft orbit, in conjunction with a laser altimeter, will be used to determine the tidal flexing of Europa and provide key information on the internal structure and nature of possible subsurface oceans.

Spacecraft lifetime in orbit at Europa is severely constrained by the radiation environment so a high data rate downlink is needed to return all of the surface imaging mapping data desired within the expected lifetime of the mission. This environment drove the need for high data rate communications on the spacecraft and to the ground.

Pluto/Kuiper Express

Pluto is the only planet in our Solar System which has not been explored by a spacecraft. Pluto and it's large moon Charon form a binary system which has an orbit varying dramatically in distance from the Sun. Currently, Pluto's orbit is within the orbit of Neptune, but 124 years hence, it will reach an aphelion of 49 AU. This variation in orbital distance causes Pluto's atmosphere to sublimate (or condense) as the distance alternately decreases and increases from the Sun. Characterization of the Pluto/Charon system will help answer questions about this unusual binary system and will contribute to our understanding of the formation of our Solar System.

After a fast reconnaissance flyby of the binary system, the trajectory will be altered to fly by a member of a group of objects referred to as the Kuiper Disk Objects. These small objects form a disk around our Solar System and are believed to remnants of the formation of the Solar System and the primary source of short period comets. By studying at least one of these objects, scientists hope to learn more about the possible origin of the volatiles which form the Earth's atmosphere and oceans.

The extreme distance from the Sun, long lifetime and fast flyby speed make this a very challenging engineering mission as well as an exciting science mission. About 2 Gb of data is expected to obtained during the few hours of the Pluto primary encounter. This will be stored onboard for transmission back to Earth during the weeks following encounter.

Solar Probe

Solar Probe is an exploratory mission to our star, which gives us life and whose effects on the earth and solar system are profound. We are only beginning to understand the relationship between the sun, its atmosphere (the corona), and the solar effects on the earth. The recent observatory missions (YOHKOH and SOHO) have given us new data to answer old questions and create new questions that can only be answered by the Solar Probe. The mission is designed to take scientific instruments into the solar atmosphere to within 3 solar radii (2.1 Gm) of the Sun's atmosphere where they will make measurements to determine what causes the heating of coronal particles (to well over a million degrees), as well as what are the sources and acceleration mechanisms in the solar winds. The low altitude passes of the Solar Probe spacecraft over the polar regions will allow imaging that has here-to-fore been impossible and at perspectives that will never be attained from near Earth observatories.

This close approach to the Sun requires that several technical challenges be undertaken. Materials in the exposed portions of the spacecraft must survive the extreme temperatures during the encounter with the Sun. The trajectory uses a Jupiter gravity assist maneuver to provide the unique quadrature geometry at perihelion. The electronics must survive the extremes in solar radiance between the dim cold of a Jupiter gravity assist flyby and the extreme heat of a close encounter of the sun.

New Millennium Space Technology 4

The New Millennium Space Technology 4 mission was a challenging journey to rendezvous with Comet Tempel 1, land on its surface, recover a sample, and possibly return it to the Earth. The Lander module contains most of the flight system avionics, plus comet surface science, anchoring, and sample acquisition equipment in a separate module on the Lander. After arrival at the comet, the flight system will go into orbit around the nucleus, and the Lander will separate from the Orbiter module, set down on the surface, anchor itself, and conduct a series of science experiments, including the acquisition of some samples. During surface operations, the orbiting module is in a passive spin stabilized mode, with its High Gain Antenna (HGA) pointed at the Earth, so it can serve as a radio relay for the Lander.

At the completion of surface science, the Lander would have jettisoned its anchoring module, left the comet surface, and rendezvoused and docked with the spinning Orbiter module. The samples would have been transferred to an Earth return entry capsule. Then the entire flight system, under control of the attached Lander module, would revert to full attitude stabilization, power up the ion thrusters, and return to Earth. Just before arrival, the flight system will put the Earth entry capsule into the correct corridor, and then jettison the capsule for recovery on Earth.

The Lander had severe mass limitations, so was to be highly optimized, both structurally and functionally. The plan was to use a pared down single string version of the X2000/IFDP avionics system.

Mars Missions

At the time when X2000/IFDP was developing its requirements there were two Mars missions on the books that were potential customers of the advanced avionics system. They were a Mars '03 Orbiter and a Mars Ascent Vehicle.

The Mars '03 orbiter was planned to be a simple bare bones communications relay for the ambitious landed science package in the Mars '03 mission. A pared-down single string version of the X2000 avionics was to be used. Extreme low mass was necessary to minimize the cost of the launch vehicle for the mission.

The 2004 Mars Sample Return mission was to be one of the most challenging interplanetary ventures of the early 21st century. Even more so than the '03 orbiter, extreme measures were to be taken to minimize mass to perform the mission with a launch vehicle small enough to fit within the cost cap. The Ascent Vehicle is the most mass critical, since all of the propellant required to boost it back into Mars orbit must first be soft landed on the Martian surface. A pared down single string version of the X2000 avionics was to be used.

Space Interferometry Mission

The Space Interferometry Mission (SIM) will determine the positions and distances of stars several hundred times more accurately than any previous program. This accuracy will allow SIM to determine the distances to stars throughout the Galaxy and to probe nearby stars for Earth-sized planets. The SIM flight system consists of the interferometer instrument systems and the spacecraft system. X2000/IFDP was looking towards the interferometer instrument system as a potential customer.

The SIM instrument is a set of optical long-baseline Michelson stellar interferometers that will acquire and track fringe patterns resulting from the interference of starlight directed along different paths. The SIM design uses three collinear interferometers mounted on a 10-meter long boom. Each interferometer collects light from two paired siderostats and combines them. Two of the three interferometers will acquire fringes from bright guide stars in order to make highly precise measurements of the spacecraft attitude. The third interferometer will observe the science targets and measure the target positions with respect to an astrometric grid of many thousands of stars distributed around the celestial sphere.

The SIM mission is an extremely challenging mission. The SIM instrument will need to operate with limited intervention from the ground, and therefore must perform important functions with a high level of autonomy and reliability. These functions include initial optical alignment, calibration, stellar target acquisition, angle tracking, fringe tracking, slew, and diagnostics. The Real-time software will play the central role in performing these functions. All of this requires a system that can provide a high computing capability and fast communications between the interferometers.

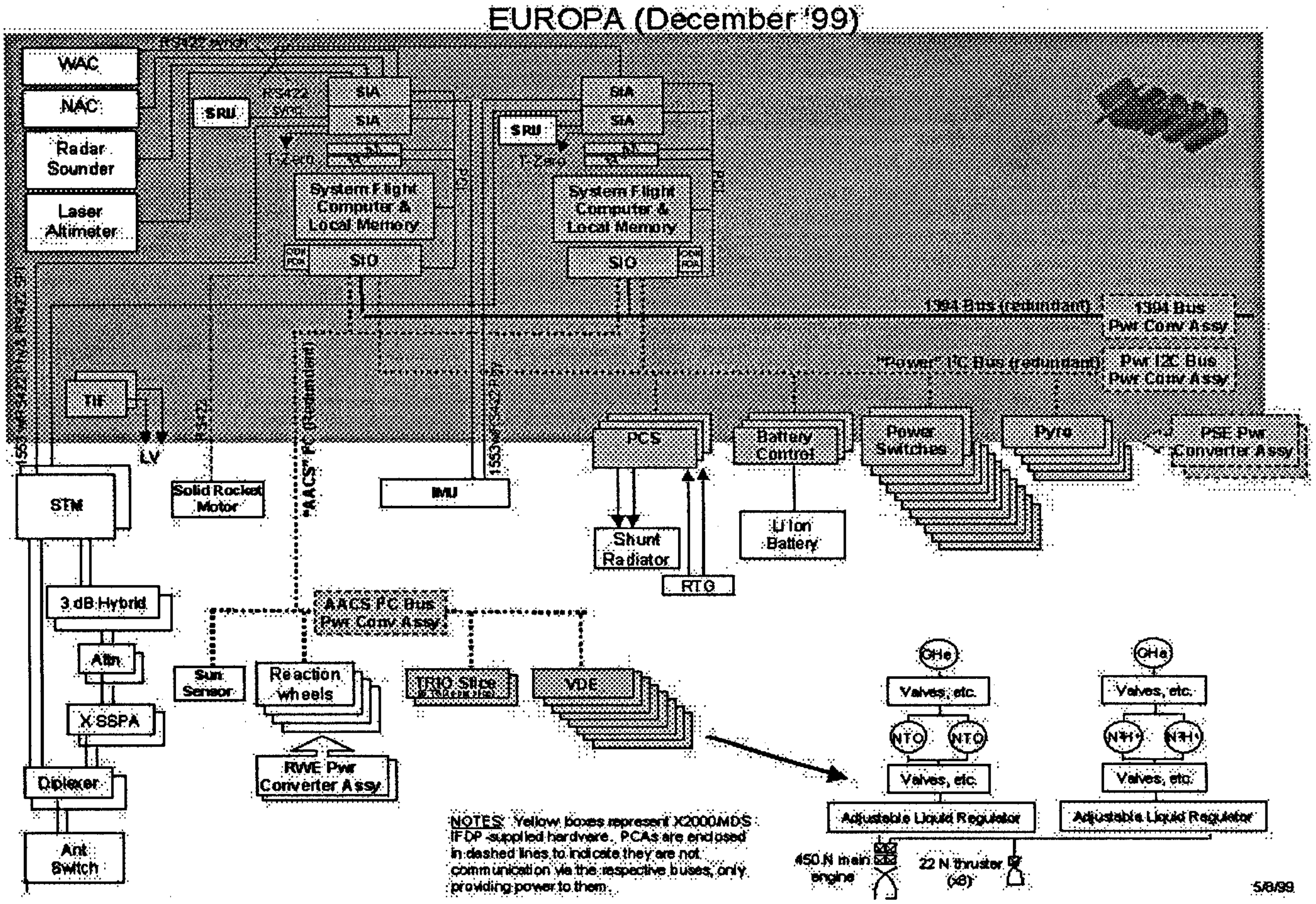
4. X2000/IFDP SYSTEM DESCRIPTION

The X2000 hardware has been developed to support multiple mission types. The architecture is capable of being modified to meet the needs of a variety of mission requirements. The X2000 hardware architecture consists of a Command & Data Handling (CDH) subsystem, a Power System Electronics (PSE) subsystem, Temperature Remote I/O (TRIO) device for capturing engineering data, and systems buses for allowing other mission unique electronic devices to be connected.

The EO instantiation of the current X2000/IFDP system architecture is shown in Figure 1.

Command and Data Handling System Description

In the CDH Subsystem the System Flight Computer (SFC)



NOTES: Yellow boxes represent X2000MDS IFDP-supplied hardvare. PCAs are enclosed in dashed lines to indicate they are not communication via the respective buses, only providing power to them.

Figure 1: Current X2000/IFDP System Architecture

is the PCI bus master and main system processor. The other CDH components attach to the SFC via the PCI bus. The other boards in the system are the Non-Volatile Memory (NVM), the System Input/Output (SIO), the T-Zero Interface (TIF) and the System Interface Assembly (SIA). The CDH provides system IO for science instruments, Attitude Control System (ACS) sensors, Telecom Systems, and other mission unique electronic components. The CDH also controls the PSE via the I2C bus.

The SFC is the main system processor and the PCI bus master. The SIO is the interface between the SFC and the two system serial buses. The Nonvolatile Memory (NVM) is a flash memory device which provides system memory capability. The System Interface Assembly (SIA) provides an interface to the telecom system and four serial connections to ACS or science instruments. The T-Zero Interface (TIF) provides an interface to the launch vehicle and launch complex equipment.

Power System Electronics Description

The PSE subsystem controls the primary and secondary power source(s), provides secondary power to spacecraft components, controls pyro devices, and commands valve actuation. The CDH provides the main source of system level control for the PSE. The PSE is capable of taking independent action during Power-On-Reset (POR) events and under fault scenarios. The PSE consists of the Power Switch Slice (PSS), Power Converter Assembly (PCA), and the Power Control Slice (PCS).

The PSS controls power switches for loads, controls pyro events, and actuates valves. The PCA provides secondary power for loads. The PCS controls the primary power bus which can be driven by a solar array or a nuclear power source.

System Interconnect Description

The architecture relies on the use of two distinct serial buses for system interconnection. These two buses work together to form the back bone of the X2000 architecture. The CDH also uses a PCI bus as the backplane bus to connect the main processor to the rest of the CDH system.

The IEEE-STD-1394 bus is a high speed (100 Mbit/s) bus for use in communication between intelligent nodes (processors). The main use of this bus is for exchange of data and health information between processors. In the configuration for EO the only nodes on this bus are System Flight Computer (SFC) which attach to the bus via the System Input/Output Assembly (SIO).

The I2C bus is a low speed (100 kbit/s) bus used to communicate between less intelligent nodes. This bus is used for commanding the Power System Electronics (PSE), collecting engineering data, and configuring the 1394 bus. There are different types of devices which interface to one another on the I2C bus. Each device can be a master or a slave on this bus depending on their capability. In the current system the Digital I/O (DIO) ASIC on the SIO is the only bus master. The Command Interface ASIC (CIA), the Temperature Remote Interface (TRIO), and EO ACS components are slaves on the bus.

5. SYSTEM RISK MANAGEMENT PROCESSES

This section will describe some of the main processes that were used by the system engineering team on X2000/IFDP. This section will provide an overview of the risk management processes utilized on the X2000/IFDP Project. Many of these processes were different than had been used traditionally on Jet Propulsion Laboratory (JPL) projects. These process changes were necessary due to the requirement of balancing technology development risk against the need to deliver a usable flight system to mission customers. Typically, technology development has not been as closely linked to flight projects as is the case for X2000/IFDP.

Risk Management versus Risk Reduction Process

Traditionally projects have dealt with risks by trying to reduced their impact as they are encountered. This can create a reactionary environment in which each risk reduction decision is handled independently only as risks occur. The overall system impact of these combined decisions is unmanaged and can often have a net cumulative negative system impact.

The risk management strategy employed by the X2000/IFDP systems team is much more proactive and seeks to minimize the overall system risk. The process involves a constant evaluation of all of the possible threats or risks to the system before they are actually manifested. This early identification of each potential risk allows for the nature of the risk (schedule, technical, cost, etc.) to be better quantified for impact and likelihood. Each risk is also evaluated to understand when and what type of a decision must be made to retire the risk. A decision gate tied to a particular event occurring or a point in time is set for each risk. The criteria for making the decision to implement a risk reduction strategy is clearly defined and agreed to prior to the decision gate occurring. An evaluation of the most likely risk management decision on the system can also be made to understand the possible impact of each potential decision. When the defined decision gate is reached an evaluation is performed based on the predetermined criteria and final decision is made. This process allows for a fully thought through system level solution to be achieved.

An example of this process was the decision to eliminate the microprocessors from the architecture. A evaluation of the development risk was made and a decision gate based on a demonstration of technology by a point in time had been established as the decision criteria. When that gate was not passed it was a logical decision to halt the development process.

Capability Requirements versus Traditional Requirements

Traditionally, system design and architecture is managed through controlling the requirement process. The system engineer can base design and architecture decisions on the need to meet the requirements which the system is designed to meet. This was not the case for the X2000/IFDP systems team because of the many often conflicting mission customer requirements. The process employed by the systems team was to manage the system capability.

The multi-mission aspect of X2000/IFDP architecture created the need for the systems team to manage the architecture and design to meet capabilities first and requirements second. Each of the missions that were relying on the X2000/IFDP system had a large divergence in mission requirements which made the system capabilities more important than the system requirements when considering possible changes to the design or architecture. The actual intent of the system requirements were what was managed as opposed to the actual requirements.

The main impact of capability management versus requirement management was to allow more fluidity of the requirement set. This lead to a better understanding of the underlying source and need for each of the requirements. This also necessitated the involvement of the mission customers in evaluating impacts to system capability when possible capability or requirement changes were considered. The capability of the architecture was used to track the development of the architecture but the traditional requirements change process was utilized for configuration control of the architecture.

A major goal of the systems team was to maintain the multi-mission capability of the architecture. Some decisions required the mission customers to compromise on their initial requested set of requirements so that other missions would have the necessary system capability. When a compromise in requirements was necessary the systems team would work with the impacted mission customer to find an alternative system solution. Through this process the capabilities of the X2000/IFDP system could be maintained so that each mission customer could meet their mission level requirements.

System level Trade Studies

On more traditional projects, trade studies consider only one or two major factors when collecting and evaluating information. Often times this can lead to a solution being selected based on an incomplete knowledge of the impacts. For example, if performance is the major factor in evaluating potential solutions then those solutions which may offer only adequate performance at lower cost, risk, or power than the higher performance options may not be considered. For X2000/IFDP, the system team process for trade studies included more of the solution space by considering all factors equally while gathering information. There was only a minimal amount of pre-screening of information during the information gathering stage of the trade study process.

Trade studies performed for the X2000/IFDP project considered all the major decision factors for each trade study undertaken. The design approach used in conducting trade studies used the following set of guidelines:

1) Make substantial use of new technologies and architectural/development concepts. This included using rad hard digital and mixed signal ASICs, flight computer with high processing capability, flash non-volatile memory, high density DRAM, and high and low speed data buses.
2) Balancing new technologies and concepts against schedule and resources.
3) Developing architectural concepts to accommodate the known set of mission required capabilities.
4) Developing an architecture and concepts that are robust and reliable. This means being single fault tolerant and having no fault propagate to redundant elements due to grounding, packaging, trace layouts, etc
5) Practice risk management, as opposed to risk reduction.
6) Maintain a standard core capability from which our customers can scale and maintain a flexible set of building blocks which our customers can tailor to their needs.
7) Minimize the number of different architectural entities (types of buses, NVM, processors/microprocessors, etc.)
8) Minimize cross-strapping
9) Develop a design that is testable in a variety of testing environments (i.e., at JPL, a contractor, launch site, etc.).

Priorities for the trade studies were identified and included performance, cost, schedule, testability and reliability. Each trade study undertaken considered all of these factors in coming up with a system solution. This required forming multidisciplinary team to be formed for each trade study so that each of the factors could be weighed equally. This process gave the project a full system impact on which to base the decision.

The approach taken by the systems team was to consider all of the decision factors in each trade study on a loose prioritized basis. For each study a trade matrix would be used which accurately identified the options and the associated impact of each one. The relative priority of the decision factors could be loosely set on the outset of the trade study to eliminate only the most improbable options.

The full set of trade study results with the options and associated impacts could then be presented to the project management for a decision. Limited filtering of the data allowed the project management leeway in selecting the weight to apply to each of the factors in the trade. This process also allowed for balanced solutions because having a complete set of impacts for each trade decision allowed the system impacts of the sum of many decisions to be more apparent. This also made it easier for the project management to manage the risk across the development.

This process will be discussed in greater detail below.

Multidisciplinary Systems Engineering Team

Typically, JPL projects have had separate teams of system engineers each working at a specific requirement or design level. Each of these teams would be responsible for a particular aspect of the development process with their own team lead, their own team meetings, their own team processes, etc. This is inefficient and can lead to confusion of roles which allows issues to be overlooked. The system team approach used by X2000/IFDP attempted to overcome this hurdle by creating a single multidisciplinary system engineering team which spanned the full technical breadth and depth of the project.

This single integrated system engineering team contained engineers with a wide variety of system engineering experience. The singular nature of the team eliminated any organizational barriers to achieving solutions and fostered a more creative environment because of the wide diversity in breadth and depth of experience. The single team was also able to eliminate duplication of function and operate more efficiently. Having a single system engineering entity enhanced the communication level between the system engineering team and the rest of the project as the systems team was solely responsible for the overall system. This increased communication made possible the early identification and resolution of many issues.

This multidisciplinary team was further enhanced as needed by adding hardware and software designers, test engineers, and fabrication engineers. This additional personnel was especially valuable while performing trade studies. Also, having the system engineering team, the implementation team and the mission customers all participating in the decision process created a mutual understanding and commitment.

System Decision Documentation Process

The system engineering team electronically documented all key project level decisions in the project electronic library. This library was available to all project members and mission customers. Each time a major decision was made or a trade study was completed the results and supporting material was archived. Included in the archived material would be at a minimum the reason for initiating the study, the participants, the key assumptions that went into the study, the data obtained from the study, the resulting decision and the rationale for the decision. Having this data archived eliminated the need to repeat completed trade studies.

The ready availability of the data also provided a clear and consistent description of the current project baseline. All of the incorporated and possible system changes were constantly available to the full team to understand and evaluate. Also members of the team always had the most up to date version of the baseline to use for understanding the current direction of the project.

6. SYSTEM PROCESSES DESCRIPTION

This section will describe the details of the main processes that were used by the system engineering team on X2000/IFDP. Each of the processes described in this section inherently employed the risk management processes described in the previous section. How each of the specific processes employed these risk management processes will be explored using examples of system processes from the different progressive phases of the project life cycle.

Initial Systems Requirements Capture Process

The key and driving requirements captured from surveying the potential customers identified are summarized in Table 1. The ultimate set of requirements accepted by X2000/IFDP were selected using a number of criteria:

1) The technological advancement desired and the budget available to achieve it
2) The capability available or predicted to be available within the time of the launch of the surveyed missions
3) The unique mission drivers that were potentially enabling for EO

In order to select an agreed upon, configuration controlled set of requirements that could be flowed down into lower level requirements, high level requirements were collected from the potential mission customers discussed earlier. Requirements from customers with which X2000/IFDP had an actual Memorandum of Understanding (the Outer Planets/Solar Probe missions (which were EO, PKE and Solar Probe) and ST4) had a bit more weight. Still, other customers had a key role in the definition of the X2000/IFDP high level requirements since two of the key tenets of X2000/IFDP were to enable/support low cost development and delivery of deep space missions and to provide multi-mission support.

System Requirements Evolution

The system architecture of the X2000/IFDP project has undergone a number of major changes over the course of the project life cycle. The original architecture was highly distributed utilizing microprocessors communicating across a high speed 1394 serial data bus. This architecture was very flexible and allowed for distributed data and command processing within each device type. This would allow science data processing to occur within the science instrument and uplink/downlink processing to occur within the telecom system.

An example of EO mission using this architecture is shown below in Figure 2.

KEY REQUIREMENT	IMPLICATION	SOURCE
Multi-mission support	Develop architectural concepts to accommodate the know set of mission needs.	Project
10 Mrad of radiation behind 40 mils of Al at electronics chassis with RDM of 1.5	- Drives cost across the system - IFDP EO suite mass driver (shielding) - Places significant constraints on components selection, increased development risk	EO
High speed data transfer capability between nodes	Drove 1394a bus selection and development for space applications	EO
High total non-volatile data storage capacity (combined with cPCI low volume physical requirement and cost constraints)	- Drove to use of high density NVE, non rad-hard - Drives mass	EO
High efficiency power conversion	- Drives development of PCM (cost and resource driver) - Technical risk increase, especially when combined with other constraints of EO mass and radiation	EO
Scaleable 1 to N computer architecture, operable all at once or single string	- Drove criteria for mult-master capable system buses - Requires new approach to prime select methodology (since it's more than 2)	Project
Flight system design that supports distributed environment	- Enables expandable/scaleable design - Allows operation in high processor margin environment, potentially saving significant SW development and system analysis time/cost	Project
100 kg mass allocation	Component selection constraint, especially when combined with radiation requirement.	EO
Configuration independent	Fault protection needs to work in any legal hardware configuration	Project
During flight, want to be able to continue operations in the face of serious and/or recurring faults	Must detect and respond to faults at lowest level so no pertubations seen in higher level software.	EO/PKE

Table 1 : Key System Requirements

This architecture was not to be realized due to major difficulties in developing a 1 Mrad microprocessor. The microprocessor was the major building block of this architecture around which the rest of the system was built. A risk evaluation was performed and a decision gate based on a decision criteria of demonstration of specific technology milestones had been established by the project. The development effort was not able to achieve these milestones by the decision gate. While this architectural paradigm of distributed processing was highly desirable it was not achievable within the budget and time constraints of the project.

This caused the project to undergo a major architectural change impacting all of the missions supported by the X2000 project. The architecture went from microprocessors distributed across the high speed 1394 serial data bus to a centralized block redundant cross-strapped system. The goal in creating this new architecture was to maintain the capability of supporting microprocessors connected on the 1394 bus for future missions. While the basic capabilities of the X2000/IFDP system were maintained, the system level requirements underwent significant revision.

Major System Requirements Change Process

The system engineering team worked closely with each of the mission customers during the process of developing an alternative architecture to the one based on microprocessors. A multidisciplinary team was formed which was made up of system engineers as well as hardware and software designers from both the X2000 project and the mission customers. This team was chartered with establishing a new architecture which maintained the basic tenets of the X2000 architecture previously defined in section 2. The team was allowed to evaluate each of the driving system level requirements to provide some trade space in which to develop the new architecture. The key component of the overall process was to maintain system capability but to allow specific requirements to change if necessary.

daily basis with the team leads convening each day to discuss what had transpired during their team meeting. This frequent meeting among the sub-team leads kept all of the other team leads aware of what possible changes were come in each area. This allowed their impact on the other sub-teams to be immediately discussed. The teams could then all understand the impact of their changes to the overall system and either incorporate the changes or modify the suggested change until it was amenable to the other teams.

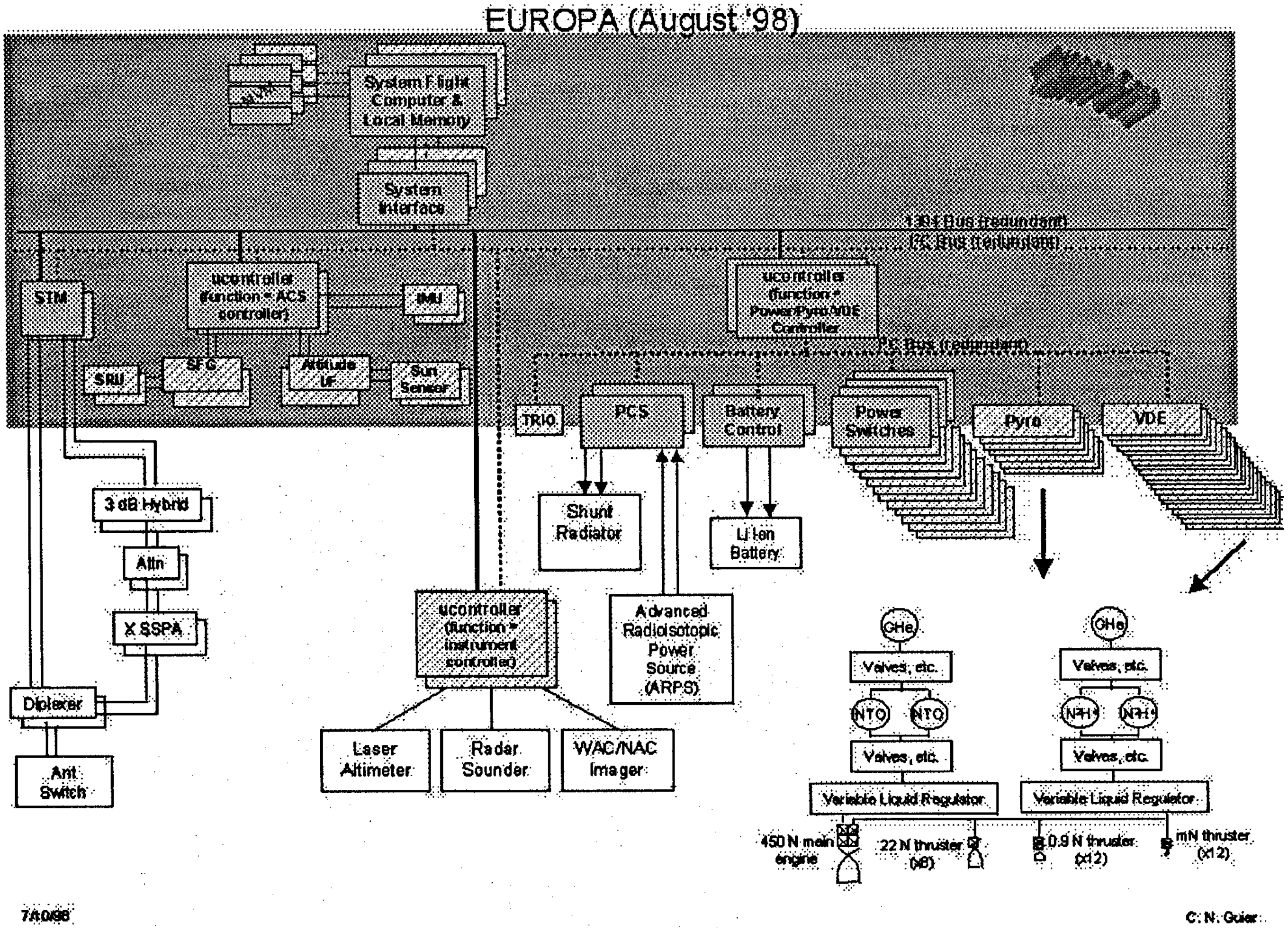


Figure 2 : Original X2000/IFDP System Architecture

One of the major factors the team considered in developing the new architecture was to reduce the technical and schedule risk of any changes. The reason for the architectural change was accumulated risk had made the initial architecture unlikely to be developed. The team was to make risk reduction a major factor in all of the trades that went into the requirements change process.

The process that was used was to subdivide the architectural team into smaller sub-teams, each of these teams then looked at a specific issue raised by the elimination of the microprocessors. The sub-teams met on a

Through this process the architectural team was able to establish a new system architecture within a few weeks. This architecture (Figure 1.) was then presented to management with all of the possible options and their associated impacts clearly defined. After management approval, work was begun on developing this new system architecture.

System Redefinition Process

In April of 1999, a working group was convened to generate an implementation plan, with supporting schedules and reporting matrices, for the delivery of the

X2000 Core Delivery to the user missions. Up until this time, there was no clear roadmap for pulling together the hardware and software products being developed and delivered by separate organizations into a consolidated package. The Core Delivery was defined to be an integrated product consisting of:

1) X2000 Core Hardware - The defined X2000 hardware configured to match mission needs in terms of quantity and interconnection.
2) MDS/X2000 Baseline Software Delivery - The software to be delivered with the X2000 core hardware as a defined, integrated and tested package. The baseline software will demonstrate the viability of the integrated product (X2000 Core Delivery) to meet customer needs and allow for mission specific modification/adaptation without significant, unplanned impact upon the customer.
3) Supporting hardware, software, and documentation that is required to provide a "complete" X2000 core integration and test environment from which the used missions continue their development efforts.

Neither Flight Software Acceptance Testing or Hardware - Flight Software compatibility testing was included in any of X2000's plans. During the time of this working group, the test program for X2000 was enhanced to include System Core Acceptance Testing (SysCAT) for reducing risk in this area, the charter of which is to demonstrate/validate the integrated product and certify its readiness for delivery to the user missions. SysCAT was envisioned to have the following characteristics:

- Independent of MDS software developers
- Formally verifies X2000 and MDS requirements at an integrated product level.
- Team may migrate to missions or MDS after X2000 Core Delivery, transferring their corporate knowledge with them
- Does not verify hardware only requirements
- Demonstrates a viable, integrated product

Trade Study Case Study

This section will trace the evolution of the development of the System Interface Assembly (SIA) from its inception late in the project to its current state. This case study will show the details of how some of the system engineering processes' were employed.

After the architectural change eliminating the microprocessors it became necessary to add a new device to the architecture to interface with the science instruments, attitude control sensors and telecom device. This card ultimately became called the System Interface Assembly (SIA). This card effectively replaced the microprocessor as the interface between the System Flight Computer (SFC) and the science instruments, sensors, and telecom system.

The process of determining the requirements for this card was somewhat different than had been employed previously for the other system components. The prior process had been that the architecture paradigm of a highly distributed and flexible system had driven the requirements of the components. This had been a top down process in which the design of the system had been worked prior to defining the components. There had also been a fairly long period of time in which to define these components.

The process that was implemented for the SIA was more of a bottom up design effort. The higher level requirements of what the card needed to do at the system level were defined to be simply provide equivalent interface capability as existed for the microprocessors. This is a good example of how the necessary capabilities drove the requirements.

The goal of the definition team was to try to keep the card as flexible as possible while defining the interface requirements. This activity needed to be completed in a relatively short period of time to keep to the project schedule. The team was also tasked with minimizing the development risk.

To achieve this goal a small multidisciplinary team of X2000/IFDP and mission system engineers, hardware designers and software designers met over several weeks to define the SIA requirements. The charter of the team was to define a set of detailed requirements for the SIA so that the designers could begin the design process and the mission customers could begin specifying interface characteristics to science instrument providers. This required that the team define the interfaces and the processing requirements for this card such that it met the large set of possible mission customers.

The goal was to come up with a flexible commercial off the shelf (COTS) serial interface protocol using RS-422 drivers which could be used to communicate with most of the defined mission instruments and attitude control sensors. Those sensors or instruments which could not be accommodated by the SIA COTS interface would be placed on one of the system buses or an available Universal Asynchronous Remote Terminal (UART) interface. The decision to use a COTS interface was made to make the flight and ground software and hardware development easier. The team felt that a COTS interface would significantly reduce the development and test risk as there were to be many disparate development efforts performed in parallel.

During the SIA requirements definition process the team developed the driving factors in ultimately determining the interface requirements. These driving requirements were arrived at through a process of fact finding and then negotiation between the affected systems. Instead of establishing a set of system requirements and waiting for the hardware and software designers to begin to implement these before possible issues were identified a more proactive approach was taken. The goal was to work the design solutions to a sufficient detail to know that the hardware and software designers had a clear understanding and agreement on the required system capabilities. This required that the multidisciplinary team had to develop a design to a sufficient level to define the driving requirements on the SIA.

First the set of driving requirements and system resource constraints were defined. The mission customers defined what the data rates and processing requirements were for their science instruments and ACS sensors. The hardware designers described what the physical constraints of fitting desired capability within an ASIC mounted onto a Compact PCI form factor board. The software designers defined what the acceptable processing impacts and resource availability were to allow them flexibility in designing the software system. After these various requirements and constraints were clearly identified the capabilities of the SIA were negotiated.

There were a set of four driving requirements defined through the negotiation process. The first driving requirement was to assume that the science instruments would do minimal or no data processing and that they needed to get their data to the SIA as quickly as possible. This requirement came from the high radiation Jovian environment and the difficulty of providing 1 Mrad devices to all of the potential vendors and instrument providers. This drove the speed of the data interface to be 6 MHz to allow fast data transfers. The second driving requirement was for the SIA to accommodate enough interfaces to enable each of the missions with some margin. This requirement drove the design to have interfaces to four external (science or attitude control) devices on each card. The third driving requirement was to limit the software overhead for servicing SIA interrupts. This requirement came from the concern that all of the data processing requirements transferred from the microprocessors to the SFC may be an excessive burden if there were more than 10 interrupts per interface per second from the SIA. This drove the size of the SIA Buffer memory to be sufficiently large enough to buffer all four high rate channel simultaneously. The fourth driving requirement was to make the interface design flexible enough to be used for multiple missions. This requirement came from the fact that the X2000/IFDP project has been chartered to support a wide variety of mission types many of which are still undefined. This requirement drove the overall architecture of the card.

There were some other assumed capabilities for the SIA card. The SIA card had to contain enough functionality to effectively replace the interface capability of the microprocessors. Also, the SIA interfaces should be standard COTS serial interface. Previously the instruments or sensors communicated with the microprocessor across a serial or parallel data link. Now all of these devices would use a standard serial interface.

The Telecom System interface was the exception to this standard COTS serial interface. The SIA was initially designed to interface with the Space Transponding Modem (STM). The STM is a next generation telecom system being developed at JPL for future spacecraft and was baselined for use by the mission customers. The STM interface utilizes a 1553 bus protocol implemented as a point-to-point RS-422 physical link for engineering and mode control. The STM also has separate SPI interfaces for command and telemetry links to the CDH.

The STM is a light weight and capable device which includes within it much of the processing historically performed by the Command and Data Handling (CDH) system. This shift in command and data processing responsibility from the CDH to the STM changed the fundamental interface between the two systems.

Previously, the Telecom System, most recently implemented as a Small Deep Space Transponder (SDST), would provide command streams to the CDH Hardware Command Decoder (HCD) which would validate the commands prior to forwarding them to the main computer. Similarly, the Reed Solomon Downlink Encoder (RSDL) within the CDH would encode the telemetry frames which the CDH would then timestamp prior to transmission to the SDST for downlink to the ground. Conversely, the STM contains the HCD, RSDL, and Timestamp functions fundamentally changing the level of the interface between the two systems. The STM also has the capability to do Turbo Encoding on the downlink data. Even though the functionality of the devices were different the STM and the SDST shared the same interfaces to the CDH.

Part way into the definition process of the SIA the project gave new direction to requirements definition team. The team was requested to determine the best way to incorporate an interface to the SDST in addition to the STM. This caused the team to instigate a trade study to determine the most effective method of achieving all of the previously defined requirements while incorporating the additional requirements.

The process for resolving this trade study was similar to what had been done in the past by the systems team. A multidisciplinary team was formed to conduct this trade study and make a recommendation to the project on the project management on how to implement these new requirements. In the end there were two options that were considered viable and both were presented to the project. The unique aspect of this trade study was that the trade study team did not arrive at a consensus in the team as to the best option. As a result, each of the affected areas (software, test, hardware design, mission customers, and systems) each provided their impact assessments as well as a recommendation as to which option they preferred and a rationale. The systems team provided a synopsis of these to the project so they could make the decision. This process worked well as each of the team elements were able to provide their independent assessment and defend their recommendation. This process allowed for the best project wide decision to be made without alienating any of the elements. At the conclusion of the effort all of the elements supported the final project decision even if they had not recommended it initially.

System Verification Process

The verification process can be divided into a short loop and a medium/long loop.

The short loop consists of the following elements:

1) Requirements Review & Signoff
System and subsystem engineers review lower level requirements document and make sure it is consistent with the higher level requirements. In addition, Level 3 and 4 requirements documents have gone through a presentation review cycle with both internal and external representation prior to final document submission for signature.

2) System Engineering In The Loop (informal, difficult to document)
Design discussions, system and subsystem engineering overview of design as it matures, helping clarify ambiguous or difficult to interpret requirements, double checking to make sure design meets intent of requirements. Also, working w/ designers as they generate detail requirements and specs to verify description is adequate.

3) Verification Matrix Generation
X2000 Flight Systems Engineering is responsible for Level 3, Level 4, and Software Verification Matrix generation. During the course of defining the verification requirements for each requirement line item, another defacto layer of requirements review is introduced into the process, providing a forum for Cognizant Engineers, system engineers, and I&T engineers to discuss the requirements text as well as the most appropriate verification method. Often additional requirements changes are identified during this process.

The medium/long loop consists of the following:

1) Formal PDRs and CDRs - Project, Element, Subsystem, Card, ASIC level
Provide forum for internal and external review of design. Customer and project system and/or subsystem engineers are present. Design details inconsistent with requirements and intended use of component are identified and corrected via RFAs, or, accepted and changes flowed into rest of system to compensate.

2) Peer Reviews
Similar to formal reviews called out above but to a deeper technical level.

3) Requirements Linking / Tracing
The X2000 system engineering team plans on completing linking of level 2, 3, and 4 requirements. This will serve to identify / highlight childless high level requirements, etc., allowing another opportunity to catch requirements errors. This linking task is scheduled to be completed by December 2000.

4) Hardware Test, Software Unit Test, and System Test
Problem reports are written when the design does not meet the requirements. Also, as team learns how the system really works, system engineering is responsible to make sure system meets intent of requirements. If not, change hardware / software, or take account of behavior and document it for operational planning purposes. Prior to actual testing, test plan generation and test procedure review provides a forum for checking requirements consistency, clarity of intent, etc.

5) Design Analysis
As the design matures, systems and design engineers complete worst case analysis to see if the system or component meets key driving requirements. Analysis results are part of the requirements validation effort, feeding back into the requirements process if results indicate that requirements are too aggressive. The system engineering team works with designers to do system or subsystem level trades in order to accommodate changes to the requirements, or changes to the design, if needed. The level 3 and level 4 verification matrices call out which requirements need analysis as part of the validation and verification effort. In addition to the minimum set of analysis called out in the matrices, additional analysis is typically done as part of the design process. Both sets are used as part of the validation effort.

Together these loops provide a robust method of validation of the system.

7. Conclusion

This paper has described the difficult system engineering task undertaken by the X2000/IFDP team of trying to develop a technology rich avionics system for a divergent interplanetary mission set. The ability to balance the risks inherent in technology development against the tight

The process described for risk management had the following key aspects. First the project took a proactive approach to continually identify and evaluate potential risks before they were manifested. Early identification allowed examination of possible risk reduction options. A multidisciplinary system engineering team was developed which made for more a more effective and efficient team.

The system engineering team managed the system capabilities using the requirements as the configuration control component. This allowed the intent of the mission level requirements to remain even when the lower level requirements were changed. This allowed for a larger trade space in which to find solutions to system level issues.

Trade studies were conducted with involvement of participants from all effected areas of the project and mission customers. This allowed the system design issues to be worked in sufficient detail that the requirements and associated risks could be clearly identified. This also created a common understanding and commitment of the whole team and allowed for a much faster process.

Also all major system decisions were archived with all supporting material in the project electronic library. This created a documented rationale for each decision. This archive also provided a baseline for future trades.

ACKNOWLEDGEMENTS

The authors wish to thank the X2000/IFDP systems team for their dedication and hard work which provided much of the examples used in this paper. The authors also wish to thank Rick Grammier for the suggestions and ideas which came from his review of the draft version of this document. This work was performed at the Jet Propulsion Laboratory, California Institute of Technology, under a contract to the National Aeronautics and Space Administration.

REFERENCES

[1] Price, Humphrey W., et al, "X2000 Flight Missions Utilizing Common Modular Components", Presented at IEEE Aerospace Conference, Aspen, CO, 1998.

***Tom Hoffman** is the Group Supervisor for the Flight Systems Engineering Group at the Jet Propulsion Laboratory. He has also been involved with the X2000/IFDP project for several years first as a lead avionics system engineer for the DS-4 mission and then more recently as the Deputy System Engineering Manager for X2000/IFDP. He has worked on several successful flight projects while at JPL including Voyager, NSCAT, Cassini, and STARDUST. He has a BSEE in EECS from UC Berkeley and a MSEE in Computer Systems from University of Southern California.*

***Cecilia Guiar** is the Project Element Manager for the Systems Engineering element of the X2000/IFDP Project. She has worked on several projects at JPL, including Cassini and SIRTF and has been Group Supervisor of the Advanced Spacecraft Systems Technology Group, the Spacecraft Systems Engineering Group, and the Science Instrument Integration Group in the Spacecraft Systems Engineering section at JPL. She received her BSEE and her MSEE in Electrical Engineering from California State University, Los Angeles, and is registered as a Professional Engineer in the state of California.*